## Using Milestone XProtect<sup>™</sup> with Omnilert Gun Detect Release notes, v1.0, April 2022

1. Capabilities

Omnilert Gun Detect integrates with Milestone's XProtect video management system (VMS) to offer the following capabilities:

- Camera import directly from XProtect or through native Gun Detect ONVIF discovery. This provides a convenient way for Gun Detect to import camera information, such as camera names and geo-location, rather than adding via the Gun Detect UI.
- Bookmarking of gun detections to the appropriate camera in XProtect using "Analytics Events". The integration creates a "Gun Detected" event which can be used to trigger additional XProtect actions.
- Gun Detect integration requires the Milestone REST API which requires XProtect 2022 R1 22.1a or later.



2. Installation Pre-Requisites

Gun Detect integrates through the XProtect REST API and requires some settings in the VMS to get necessary features working. These are:

- Setup a user with admin privileges for the API
- Enable/open port 9090 to allow communications with the Event server
- Create the "Gun Detected" Analytics Event
- Setup rules and actions

## Setup Admin User

1. In XProtect Management Client, select "Security" in the Site Navigation pane and right click on "Basic Users."

Milestone XProtect Management	ent Client 20	22 R1		-	$\times$
File View Action Maintenance T	ools Help				
E 7 9 • #					
Site Navigation - •	× Basic Us	er •	Basic User Settings		- 8
Smart Wall	^	Name /	Name:		
🖻 View Groups	a me		me		
🕼 Smart Client Profiles			Description		
Management Client Profiles					
Matrix					
Rules					
Time Profiles					
Motification Profiles			Force Basic User to change password on next login		
User-defined Events			Status:		
Analytics Events			Enabled V		
Generic Events					
Roles					
System 1 & Create Basic User.	Ctrl+N				
Current Edit Basic Liser		-			
• System					
System Delete Basic User	Del				
🕹 Eviden 🥩 Refresh	F5				
Configuration reports		1			
Metedete Lles					
Metadata Search					
Access Control					
R Transact					
Transaction sources					
Transaction definitions					
a 🗷 Alarms	~				
< >					
Site Navigation Federated Site Hierar	chy		Info		

- 2. Create a username and password and deselect the box to force user to change password.
- 3. Go to "Roles", select "Administrators", and at the bottom of the screen on the right select "Users and Groups." Click "Add" -> "Basic User" -> select the user you made above. Keep note of this user and password for the REST API later

## **Enable Analytics Events**

A Gun Detect event will use the API and Analytics Events to trigger a Rule that will perform actions on our behalf, like bookmarking. The Analytics Event must be explicitly created and enabled.

1. Go to "Tools" at the top menu and click "Options"

📀 Milestone XProtect Manager	ment	Client 2022 R1			_		×
File View Action Maintenance	Tool	s Help					
日 🤊 😧 🌨 🏥	· R	edistered Services					
Site Navigation -		egisterea services.		Role Settings			• •
Smart Wall	▶ Ef	fective Roles	e	Name   Description			
View Groups	S 0	ptions Ctrl+	inistrators have	B DESKTOP-Q4M			
Management Client Profiles		Solution Provide the Providence of the Providenc	ult role created by th				
Matrix				WINT AUTHORITY			
Rules and Events							
- 🗓 Rules							
Time Profiles							
Notification Profiles							
User-defined Events							
- Analytics Events							
Security							
Roles							
& Basic Users							
System Dashboard							
Current Tasks							
<ul> <li>System Monitor</li> </ul>							
System Monitor Thresholds							
Evidence Lock							
Configuration Reports							
Metadata Use							
Metadata Search							
Access Control							
a 🖏 Transact							
Transaction sources							
Transaction definitions				Add Remove			
a 🛃 Alarms	~	1		Am			
٢	>						
Site Navigation Federated Site Hier	rarchy			🚯 Info 🗳 Users and Groups 📲 External IDP 🔹 Overall Security 🔍 Device 🕸 PTZ 🔹 Speech 🖄	Remote	Recording	S < >
_							

2. Click right on the top bar until you see "Analytics Events." Click to access that screen and make sure the "Enabled" checkbox is checked, port 9090 is being used, "All network addresses" is selected. Click Ok.

🚸 Milestone XProtect Manager	ment Client 2022 R1	-		$\times$
File View Action Maintenance	Options X			
🗄 🤊 🥹 🗢 🛍	Evidence Lock Audio Messages Privacy settings Access Control Settings Analytics Events Customer Dashboard Alarms			
Site Navigation -	Analytics events			• ņ
III Smart Wall				
View Groups				
Smart Client Profiles	Port:			
Management Client Profiles	9090			
Matrix				
Rules and Events	Security			
Time Profiles	Events allowed from:			
Notification Profiles	All network addresses			
User-defined Events				
Analytics Events	O Specified network addresses:			
Seneric Events	Address			
a 🐗 Security	•			
Roles	Import			
Basic Users				
Current Tasks				
System Monitor				
System Monitor Thresholds				
& Evidence Lock				
Configuration Reports				
R Server Logs				
a ♥ Metadata Use				
Metadata Search				
Access Control				
Transaction sources				
Transaction definitions				
a 🕏 Alarms				
<	Help OK Cancel			
Site Navigation Federated Site Hier		peech A Remote	Recording	S < >

3. Go to "Rules and Events" in Site Navigation. Click "Analytics Events" and right click on "Analytics Events" in the central window and then "Add New". Name the event "Gun

Detected" (Note: this name will matter later so ensure you correctly type "Gun Detected"). Add a description if you wish:

	1			
Site Navigation • • × Anal	lytics Events +	Analytics Events Information		<b>v</b> 0
- Smart Wall	Analytic	Chi Ni		
🖆 View Groups	Add New	Ctri+N		
Smart Client Profiles	2 Refresh	F5		
Management Client Profiles			the second s	
Sector Matrix				
Rules and Events				
🗄 Rules		Description:		
Time Profiles				
Notification Profiles				
Coser-defined Events				
Conorio Events				
Security				
- Poles				
2 Basic Lisers				
System Dashboard				
Current Tasks				
System Monitor				
System Monitor Thresholds				
& Evidence Lock				
Configuration Reports				
- A Server Logs				
⇒ 🐨 Metadata Use				
Ketadata Search				
Access Control				
⇒ 6 Transact				
- Transaction sources				
Transaction definitions				
a darms				
Site Navigation Federated Site Hierarchy				

## Rules Setup

The final piece of setup is to define a Rule -- essentially a set of actions -- that will be performed when the Gun Detected Analytics Event occurs.

1. Scroll down to "Rules and Events" in the Site Navigations. Right-click on "Rules", then "Add Rule":



 Name the Rule "Gun Detected" in the popup window. Make sure "Perform an action on <event>" is selected, and click the highlighted blue "event" link in the panel at the bottom:

📀 Milestone XProtect Manag	Manage Rule					$\times$		_		$\times$
File View Action Maintenanc ■ ♥ ♥ ♥ ♣ Site Navigation ■ © Remote Connect Services	Name: Description:	New Rule 001								¥ 8
Axis One-click Camera Co     Servers     Failover Servers     Failover Servers     Mobile Servers     Mobile Servers     Cameras     A Microphones     Speakers     Metadata      Gutput     Output     Output     Smart Wall	Active: Select the rule type yo Perform an action o Perform an action o	Ste bu want to create n <event> a time interval n a <recurring time=""></recurring></event>	p 1: Type of rule							
Site Navigation Federated Site Hill	Edit the rule description Perform an action on from devices/rec	on (click an underlined item) event ording server/management ser	ver							
	Help	Cancel	< Back	Next >	Finish		_	-	-	

 In the menu that pops up, click "Analytics Events" -> "Analytics Events" -> "Gun Detected" and click Ok

- 4. For the "From" highlighted in blue, click on the link and select the camera group you are using (e.g. "Camera Group 1"). "Add" and click Ok.
- 5. Click "Next" and "Next" again to skip the "Conditions" panel.
- 6. On the "Actions to perform" panel, select "Start recording on <devices>" and "Create bookmark on <devices>". Upon selecting, change "immediately" to the time you want (e.g. 20 seconds before the bookmark -- you do this by selecting a negative time). Select the "recording device" highlighted in blue and select "device from metadata".
- 7. Click on "Bookmark" in blue and add name/description (e.g. Gun Detect/Triggered by Omnilert Gun Detect AI). You can also click the blue highlighted items at the bottom to add metadata, for example:

🚸 Milestone XProtect Manag	Manage	Rule				_		×		_		×
File View Action Maintenanc 티 7기 영 속 해	Name:	Bookmark Details					×					
Site Navigation	Descripti	Headline										* 9
B Remote Connect Services	Descript	Gun detected on \$Dev	iceName\$									
Axis One-click Camera Co	Active:	Description										
Recording Servers     Failover Servers     Mobile Servers     Devices	Select	The event \$EventNam triggered rule \$RuleNa	e\$ was triggered at time me\$ on recording serve	* \$TriggerTime\$ on devi er \$RecorderName\$	ice \$DeviceName\$	6, which	^	^				
<ul> <li>Cameras</li> <li>Microphones</li> <li>Speakers</li> <li>Metadata</li> <li>Input</li> <li>Output</li> </ul>	Start Paus Move Set c Play											
∋	Senc						~					
<ul> <li>View Groups</li> <li>Smart Client Profiles</li> </ul>	Start			Pre-bookmark tir	me (seconds)	3	80 🗘	~				
Management Client Profile	Edit th Perfor			Post-bookmark ti	me (seconds)	3	0 ‡	- 1				
Rules and Events     Rules     email: Rules     email: Rules     email: Rules     email: Rules	fro start re and	Add system information	on (click links to insert	variables in bookmark te	ext)							
-121 Notification Profiles		Event name										
Vser-defined Events		I riggering time										
Analytics Events		Rule name										
Security		Recording server na	me									
- Boles												
<				C	ж	Cancel						
Site Navigation Federated Site Hi		Негр	Cancel	< Back	Next >		Finish	1	_	-	-	-

8. Once again select "device from metadata". Upon clicking next, you can select a "Stop Action" (e.g. stop recording 30 seconds after the event occurred.) The entire rule set should now look like the following image. Click Finish.

Milestone XProtect Management Client	Manage Rule			_	
File View Action Maintenance Tools H 同 約 ② ◆ 曲 Site Navigation •	Name: Description:	Gun Detected			
Microphones  Speakers  Metadata  Continue  Continue Continue  Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Continue Contin	Active: Select actions to per Move to default p Set device outpu Create bookmark Play audio <mes Send notification Make new <log e<br="">Start plug-in on &lt; Apply new settin</log></mes 	S rform preset on <devices> with PTZ &lt; t to <state> k on <devices> sage&gt; on <devices> with <prior to <profile> entry&gt; <devices> <devices> gs on <devices></devices></devices></devices></profile></prior </devices></devices></state></devices>	tep 3: Actions priority> ity>		^
	Edit the rule descrip Perform an action on from <u>Crest</u> start recording <u>20 sec</u> and Create bookma Perform action <u>30 sec</u> stop recording <u>immed</u>	tion (click an underlined item) <u>Gun Detected (Analytics Events</u> conds before on the devices from ark <u>Gun detected on \$DeviceNar</u> <u>conds after</u> <u>liately</u>	) I metadata me\$ on the devices from metad	ata	
	Help	<u>C</u> ancel	< <u>B</u> ack	<u>N</u> ext >	<u>F</u> inish

9. Setup is now complete. It is worthwhile to test the Event is setup correctly. You can quickly do this by clicking on "Analytics Events" under "Rules and Events", choosing "Gun Detected" and then "Test Event." Select the server, camera group and a camera to test with. You should see a bookmark show up in the live view for the selected camera.



Installation of the Milestone XProtect Plug-in

The XProtect Plugin is installed using the Gun Detect mini menu on the Gun Detect server.

- Open a terminal and start the mini menu with command "gdm"
- Select "Setup Integrations"
- You should have a list of available integrations. Select XProtect
- The installer will run and ask for XProtect credentials. These are the username and password you used when you created the administrative user earlier
- The installer will ask for the address of your XProtect server, which you can provide as a domain name or IP address (e.g myserver or myserver.company.com or 192.168.10.123).
- Provide the Port which was used, normally 9090.
- Add a location (a descriptive name of the server, site, location, etc.)
- The API currently is not capable of reliably returning information on the stream URI and port used for any cameras known to the VMS. A camera is accessed via its RTSP address which is of the form:

rtsp://username:password@server\_address:port/stream\_information

for example:

rtsp://192.168.20.4:554/mainStream01

The Stream URI in this example is "//mainStream01" and the port is 554.

Depending on how your cameras are configured, XProtect may or may not be able to provide this information for each camera. The plugin, therefore, allows you to specify a global port and Stream URI as a convenience. This is only helpful if your cameras all have the same port and Stream URI, but it can ease the work in setting up the rest of the integration.

• At this point the plugin is configured and will run to contact the XProtect server to retrieve camera information. If successful, the plugin will leave the camera file in

~/hooks/discovery/milestone-import.dat

You can edit this file to ensure the camera information is correct.

• Run "Find Cameras" within the Gun Detect UI to import this camera information. Note that if the cameras are discoverable by GD's native ONVIF scanner they may also show up on the Find Cameras list. You can disable the ONVIF scanner by creating a file "nolocal" in the discovery directory:

touch ~/hooks/discovery/nolocal